WILLKIE FARR & GALLAGHER LLP
Benedict Y. Hur (SBN: 224018)
Simona Agnolucci (SBN: 246943)
Eduardo E. Santacana (SBN: 281668)
Jayvan E. Mitchell (SBN: 322007)
Amanda Maya (SBN: 324092)
One Front Street, 34th Floor
San Francisco, CA 94111
Telephone: (415) 858-7400
Facsimile: (415) 858-7599
bhur@willkie.com
sagnolucci@willkie.com
esantacana@willkie.com
jmitchell@willkie.com
amaya@willkie.com

Attorneys for
GOOGLE LLC

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO

ANIBAL RODRIQUEZ, *et al*., individually and on behalf of all other similarly situated,

Plaintiffs,

vs.

GOOGLE LLC,

Defendant.

Case No. 3:20-CV-04688

DEFENDANT GOOGLE LLC'S MOTION TO DISMISS FIRST AMENDED COMPLAINT PURSUANT TO FED. R. CIV. P. 12(B)(6)

Court: Courtroom 3 – 17th Floor
Date: February 25, 2021
Time: 1:30 p.m.

Judge: Hon. Richard Seeborg

TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD:

Please take notice that, on February 25, 2021, the undersigned will appear before the Honorable Richard Seeborg of the United States District Court for the Northern District of California at the San Francisco Courthouse, Courtroom 3, 17th Floor, 450 Golden Gate Avenue, San Francisco, CA 94102, and shall then and there present Defendant Google LLC's Motion to Dismiss Plaintiffs' First Amended Complaint (the "Motion").

The Motion is based on this Notice of Motion and Motion, the attached Memorandum of Points and Authorities, the accompanying Request for Judicial Notice and exhibits attached thereto, the pleadings and other papers on file in this action, any oral argument, and any other evidence that the Court may consider in hearing this Motion.

ISSUES PRESENTED

Whether Plaintiffs fail to state a claim upon which relief can be granted, thus warranting dismissal of the Complaint (Counts I–VI) under Fed. R. Civ. P. 12(b)(6).

RELIEF REQUESTED

Google requests that the Court dismiss the First Amended Complaint with prejudice.

Dated: December 17, 2020

Respectfully submitted,

WILLKIE FARR & GALLAGHER LLP

By: /s/ *Benedict Y. Hur*

Benedict Y. Hur

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases **Page(s)**

Statutes

Other Authorities

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

Rather than oppose Google's initial Motion to Dismiss, Plaintiffs instead filed an 80-page First Amended Complaint bloated with irrelevant information that has nothing to do with their claims. Focusing on Plaintiffs' *pleaded* claims and the miniscule set of *actual* factual allegations concerning the bases for those claims reveals that they do not meet the requirements of Rule 12.

The claims Plaintiffs actually assert relate to alleged privacy violations stemming solely from the use by third-party app developers of a Google tool called Google Analytics for Firebase ("GA for Firebase"). The apps at issue used GA for Firebase to learn more about their users' interaction with the apps. App developers incorporated Google's analytics tool into their app, causing some data about their users' interactions with their apps to be sent to Google to be analyzed for the app developers. The apps that used GA for Firebase were required by Google to disclose to users that they had authorized GA for Firebase to receive data about user activity on the app, and they did. This case is therefore about the authorized collection of data that users knowingly provided to apps so the app developers could understand the data using Google's tool. For example, The New York Times app incorporates GA for Firebase to analyze how users interact with news content. Standing alone, there is no conceivable claim that could be made against Google for providing this tool to app developers, the use of which is premised on the consent of all involved in order to make apps better for everyone.

Plaintiffs therefore manufacture their theory of liability on the basis of a completely unrelated Google account-level setting called Web & App Activity ("WAA"). While GA for Firebase is a tool for developers, WAA is a tool for Google users. When WAA is "on," it allows Google to save a user's online searches and activity in the user's Google account to help Google provide faster, more relevant searches and other forms of personalized experiences across Google services. Importantly, while the class is limited to those who used "***non-Google*** branded mobile apps" (First Amended Complaint ("FAC") ¶ 225), WAA "saves your activity on ***Google*** sites, apps and services." *Id.* ¶ 71. There is no allegation that WAA saves the data that third-party apps authorize GA for Firebase to collect, nor could there be. Whether WAA is "on" or "off," the data

that non-Google apps collect using GA for Firebase is not stored in a user's Google account. Taking every allegation of the complaint as true, there is no alleged conflict between Google's representations relating to WAA and its analytics tool for third-party developers.

Fundamentally, every claim fails because both the app developers and their users consented to the app developers' use of GA for Firebase. As a result, there can be no plausible Wiretap Act, CIPA, invasion of privacy, intrusion upon seclusion, CDAFA, or UCL claim.

The Amended Complaint is legally deficient for a number of other reasons. The Wiretap Act claim fails even if Plaintiffs had not consented to Google's collection, because it requires only consent from one party, which the app developers obviously provided. The CIPA claim fails because the Amended Complaint does not allege that the communications are confidential. Nor can Plaintiffs state an invasion of privacy or intrusion upon seclusion claim because they have not alleged an actionable privacy interest, much less an egregious breach of social norms.

Plaintiffs' CDAFA claim is baseless, too. Plaintiffs allege that Google violated the CDAFA by collecting data from apps using software (GA for Firebase) that app developers intentionally integrated into their apps. But CDAFA requires that a defendant access data by circumventing technical or code-based barriers put in place to restrict access to the information. The complaint does not allege any such circumvention. Finally, the UCL claim fails because Plaintiffs have not pleaded that they lost money or property as a result of Google's conduct, and therefore lack standing to bring a UCL claim. Plaintiffs have also failed to state a claim under either the "unlawful" or "unfair" prong because they cannot plausibly plead a violation of any of the offenses upon which the claim is based. Having already had an opportunity to amend, the complaint should be dismissed with prejudice.

II. BACKGROUND AND PLAINTIFFS' ALLEGATIONS

A. App developers voluntarily integrated GA for Firebase into their apps.

Google LLC ("Google") is a technology company that offers popular products, including analytics and measurement software and services for websites and apps. FAC ¶¶ 21, 40, 42. The Firebase Software Development Kit ("Firebase SDK") is a Google product that helps app developers develop their apps; it includes access to Google analytics services and various other

components. *See id.* ¶¶ 40, 42. App developers use GA for Firebase as a tool to collect their users' app usage data so they can improve their experiences. *Id.* Plaintiffs muddy the relevant terminology in their complaint by using Firebase to mean both or either of GA for Firebase and the "Firebase SDK" as a whole, which includes other tools unrelated to analytics.

As alleged, if an app developer chooses to use it, GA for Firebase automatically collects certain data when a user interacts with the developer's app, including: (i) the title of the viewed page, (ii) the "page_referrer" (i.e., if the user arrived at that page via another page), (iii) the "page_location", (iv) language, and (v) "screen_resolution". *Id.* ¶ 52, 55. It can also collect other types of information, such as app browsing histories or search queries. *See id.* ¶ 241.

B. App developers authorized the sending of their users' data to Google.

Plaintiffs allege they used 444 apps on their mobile devices during the class period. But, they allege that only their "communications with *the apps that used Firebase SDK* were intercepted and tracked by Google without [their] knowledge or consent." FAC ¶¶ 206–223 (emphasis added)). Of those 444 apps, the FAC alleges that only nine of them are "supported by" the Firebase SDK: The New York Times, NPR One, Duolingo (an app that teaches users foreign languages), Alibaba (an e-commerce tool), Lyft, Venmo, The Economist, Trivago (a hotel price comparison app), and Wattpad (an app that connects writers and readers together). FAC ¶ 205. These nine apps are the only apps relevant to Plaintiffs' claims, although they fail even to allege that any particular app uses GA for Firebase as opposed to the Firebase SDK generally.[1]

App developers integrate GA for Firebase into their apps to analyze how their customers use the app, which they do by authorizing the sending of users' app activity data to Google via GA for Firebase. The GA for Firebase Terms of Service agreement ("GA for Firebase ToS") that Google executes with app developers defines Firebase as "the Firebase Software Development Kit, which *is used or incorporated in an App for the purpose of collecting Customer Data*,

[1] Plaintiffs allege that they cannot identify all of the apps that are relevant in this litigation because Google does not disclose a list of which apps use GA for Firebase, and that this information can only be ascertained in discovery. As explained *infra* § II(C), Google requires apps that use GA for Firebase to disclose its use to users. And, as illustrated *infra* § II(C), all of the apps at issue in this litigation made that required disclosure in their respective Terms of Service and/or Privacy Policies. Regardless, even if the allegation were true, it is no basis to allow the FAC a free pass.

together with any fixes, updates and upgrades provided to You." Google's Req. for Jud. Not. ("RJN"), ¶ 1; Decl. of Andrew Rope ("Rope Decl.") ¶ 2 & Ex. 1(a)–(b), pp. 2, 12 (emphasis added)). The Google Analytics for Firebase Use Policy ("GA for Firebase Use Policy") also makes clear that by subscribing to GA for Firebase, app developers authorize Google to collect users' app activity data. The GA for Firebase Use Policy states: "[b]y enabling Google Analytics for Firebase you enable the collection of data about App Users, including via identifiers for mobile devices (including Android Advertising ID and Advertising Identifier for iOS), cookies and similar technologies." Rope Decl. ¶ 3 & Ex. 2(a)–(b), pp. 1, 3; RJN ¶ 2.

C. Google required app developers to disclose the use of Google Analytics for Firebase to collect users' data and to get users' consent.

The GA for Firebase ToS requires the apps to (1) disclose their use of GA for Firebase to users, and (2) obtain their users' consent to the storing and accessing of their data by Google:

> You must post a Privacy Policy and that Privacy Policy must provide notice of Your use of cookies, identifiers for mobile devices (e.g., Android Advertising Identifier or Advertising Identifier for iOS) or similar technology that are used to collect data. ***You must disclose the use of the [GA for Firebase] Service, and how it collects and processes data***. . . .***You will use commercially reasonable efforts to ensure that a User is provided with clear and comprehensive information*** about, and consents to, the storing and accessing of cookies or other information on the User's device where such activity occurs in connection with the Service and where providing such information and obtaining such consent is required by law.

Rope Decl. ¶ 2 & Ex. 1(a)–(b), pp. 5, 14. Here, the apps at issue disclosed the collection of user data by third parties (some by specifically disclosing the use of Google Analytics). For example, Alibaba's Privacy Policy explicitly states that:

> Our Platform uses Google Analytics, an internet analytics service provided by Google, Inc. ("Google"). Google's cookies allow us to analyze use of the Platform by telling us which pages our users are viewing, which ones are most popular, what time of day our Platform are visited, if users have previously visited our Platform, from which website users are redirected to our Platform were and the like. ***The data generated by the cookie about your use of the Platform will be transmitted to Google and stored by Google on servers in the United States***.

Decl. of Jayvan E. Mitchell ("Mitchell Decl.") ¶ 3 & Ex. B(1)–(2); RJN ¶ 4. Lyft's Privacy Policy similarly states that "[w]e collect information through the use of 'cookies,' tracking pixels, data analytics tools like Google Analytics, SDKs, and other third party technologies to understand how you navigate through the Lyft Platform and interact with Lyft advertisements." Mitchell Decl. ¶ 5

and Ex. D(1)–(2), pp. 3, 16; *see also id.* p. 30; RJN ¶ 6. The New York Times, NPR One, Duolingo, The Economist, and Trivago apps also disclose the use of GA for Firebase to collect user data. *See* Mitchell Decl. ¶¶ 6–7, 10–13; RJN ¶¶ 7–8, 11–14. Wattpad similarly discloses the collection and sharing of users' app data with third-parties such as "Analytics providers." Mitchell Decl. ¶ 8; RJN ¶ 9.

Each of these apps incorporates these disclosures into their terms of service agreements, which users must agree to as a condition of using the apps. *See* Mitchell Decl. ¶¶ 2, 4 & Ex. A(1)–(2), pp. 1, 19, 40, 55, 71, 88, 104; Ex. C(1)–(2), pp. 1, 38, 80–81; RJN ¶¶ 3, 5. Thus, in addition to the apps authorizing Google's access to users' app activity data, and in addition to the fact that users are informed about GA for Firebase, the users themselves also consented.

The FAC ignores all of these terms of use, focusing instead on Google's Privacy Policy. But that policy makes clear that Google collects users' data pursuant to the consent users provide to third-party app developers. For example, Google explains in its Privacy Policy that when users provide consent to apps to let Google collect their data, Google "will respect the purposes described in the consent [users] give to the site or app, ***rather than the legal grounds described in the Google Privacy Policy. If you want to change or withdraw your consent, you should visit the site or app in question to do so.***" Mitchell Decl. ¶ 15; RJN ¶ 16. Google also discloses that another way to stop the collection of data from apps that use Google Analytics is to install the Google Analytics browser add-on: "Many websites and apps use Google Analytics to understand how visitors engage with their sites or apps. If you don't want Analytics to be used in your browser, you can install the Google Analytics browser add-on." Mitchell Decl. ¶ 9, and Ex. H(1)–(2); RJN ¶ 10.

D. Google forbids app developers from sending Google users' PII.

The GA for Firebase ToS forbids app developers from sharing users' personally identifiable information with Google, requiring that apps "will not, and will not assist or permit any third party to, pass information to Google that Google could use or recognize as personally identifiable information." Rope Decl. ¶ 2 & Ex. 1(a)–(b), pp. 4, 14. The GA for Firebase Use Policy similarly mandates that apps "will not facilitate the merging of personally-identifiable

information with non-personally identifiable information unless you have robust notice of, and the user's prior affirmative (i.e., opt-in) consent to, that merger." *Id.* ¶ 3 & Ex. 2(a)–(b), pp. 1, 3. Google also requires that where apps assign user IDs, the apps "are responsible for ensuring that [their] use of the user ID is in accordance with the [GA for Firebase ToS]. This includes avoiding the use of impermissible identifiable information and providing appropriate notice of your use of identifiers in your Privacy Policy. Your user ID must not contain information that a third party could use to determine the identity of an individual user." Mitchell Decl., ¶ 14, and Ex. M; RJN ¶ 15. The FAC makes no mention of any of this, and asserts in conclusory fashion, without specifying, that certain types of data that *are* personally identifiable were collected by GA for Firebase.

E. WAA cannot serve as a basis to manufacture a lack of consent to a third party's use of Google Analytics for Firebase.

Plaintiffs allege that app developers use GA for Firebase to send Plaintiffs' app activity data to Google without Plaintiffs' consent. *See* FAC ¶ 42(a). The sole basis for Plaintiffs' claim that app developers and Google lacked their consent is that Plaintiffs allege they turned off WAA. *See id*. ¶¶ 1, 76, 84. As the FAC demonstrates in a screenshot, Google tells users that WAA enables them to allow Google to save "your activity on ***Google sites and apps***" to "your Google account" in order to provide the users with better recommendations and service. FAC ¶ 71–73. The alleged class, however, is limited to those who used a "***non-Google branded*** mobile app." FAC ¶ 225. The FAC therefore demonstrates the irrelevance of WAA to the action.

Indeed, nothing in the FAC links WAA to the separate and independent product Google provides to app developers (*not* its users) allowing them to analyze user's interactions with *their* apps—not a Google service or app. And there is no allegation that GA for Firebase stores that information in a user's Google Account, regardless of whether WAA is on or off. Likewise, there is no allegation that if WAA were turned "on," it would store the information that apps use GA for Firebase to collect.

Plaintiffs nevertheless allege that they "had the objectively reasonable belief that Google would stop collecting their communications and other interactions with apps on their phones" if

WAA was turned off. FAC ¶ 75. That is artful wording meant to obscure the reality that is plain from the FAC's allegations, paired with various strategic excerpts from various disclosures by Google and quoted in the FAC. *See id* ¶ 70–75. This language and the source documents do not support Plaintiffs' conclusory allegation. These disclosures are about what Google stores in users' Google Accounts relating to their use of Google services. Plaintiffs cannot rely on the WAA disclosures to establish Plaintiffs' purported expectation about an entirely separate practice (the collection of *third party* app data for analytics) governed by separate disclosures.

Plaintiffs claim that language from a Google Help Center web page titled "See & Control your Web & App Activity," and the "Learn More" settings description on Android phones "explained" that turning off Web & App Activity would "prevent" Google from saving user data from third-party apps that use Google's services. *Id*. ¶¶ 70–75. As told by Plaintiffs, this language suggests that Google would "stop collecting their communications and other interactions with apps on their phones" when the Web & App Activity setting was turned off. *Id.* ¶ 75. But no reasonable person would interpret that language to mean that Google stops *receiving all data* when Web and App Activity is turned off. The webpage states that: "[i]f Web & App Activity is turned on, your searches and activity from ***other Google services*** are ***saved in your Google Account***, so you may get more personalized experiences, like faster searches and more helpful app and content recommendations." *See id*. ¶ 70, n.21 (emphasis added). This language does not suggest that turning off WAA obligates Google to prevent third-party app developers from using Google's analytics tool—a tool that app developers and users separately authorize. Indeed, Google's Privacy Policy expressly carves out independent consent given to third parties for the provision of data to Google as superseding. Mitchell Decl. ¶ 15, and Ex. N; RJN ¶ 16.

The FAC also selectively quotes Google's policies and disclosures, omitting those portions that make clear how users can stop Google from collecting user data from apps that use GA for Firebase. For example, the Google Privacy and Terms explains that:

> Many websites and apps use Google Analytics to understand how visitors engage with their sites or apps. If you don't want Analytics to be used in your browser, you can install the Google Analytics browser add-on. Learn more about Google Analytics and privacy.

Mitchell Decl., ¶ 9, and Ex. H(1)–(2); RJN ¶ 10. There is no basis for Plaintiffs to link WAA and GA for Firebase. That Google provides privacy controls for users should not be used as a cudgel to attack Google's unrelated programs for purported misrepresentations about how its privacy controls work.

III. LEGAL STANDARD

A complaint must be dismissed where the plaintiff fails to allege "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). Courts accept as true only well-pleaded factual allegations. *See Ashcroft v. Iqbal*, 556 U.S. 662, 679 (2009). The analysis begins by discounting allegations that are "no more than conclusions," and so "are not entitled to the assumption of truth." *Id.* The court also "need not . . . accept as true allegations that contradict matters properly subject to judicial notice." *In re Gilead Scis. Secs. Litig.*, 536 F.3d 1049, 1055 (9th Cir. 2008) (citation omitted).

IV. ARGUMENT

Every one of Plaintiffs' claims fails because app developers intentionally and with the consent of their users integrated a Google tool into their apps to help them analyze app usage. None of this contravenes settled expectations, users' consent, or any law. The claims also fail for five other independent reasons: (i) the app developers' consent alone exempts Google from liability under the Wiretap Act (Count I); (ii) Plaintiffs fail to sufficiently plead what data was collected, never mind how, under the circumstances, they had an actionable privacy interest in that data (Counts II, IV, and V); (iii) Plaintiffs fail to plead that collection of the app activity data was highly offensive (Count IV and V); (iv) Plaintiffs do not allege that Google circumvented any technical or code-based barriers in order to access their app activity data (Count III); and (v) Plaintiffs fail to plead that they suffered an injury in fact as a result of Google collecting their data and fail to claim that Google's collection is unlawful or unfair under the UCL (Count VI).

A. Each claim fails because Google was authorized to receive Plaintiffs' data.

Each claim fails because: (1) the app developers chose to use GA for Firebase and consented to its use; (2) Google required those app developers--as a condition of using GA for Firebase--to obtain consent from their users; and (3) the app developers obtained the required

consent. Plaintiffs' claims therefore fundamentally allege that an app developer cannot use GA for Firebase as a tool to analyze their users' activities on their own app, even with consent from those users. Plaintiffs' consent is fatal to every one of their claims. *See, e.g., In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1026 (N.D. Cal. 2014) (consent by one party defeats Wiretap Act claim) (Count I); *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 607 (9th Cir. 2020) (citing Cal. Pen. Code § 631(a) (CIPA prohibits only unauthorized interception) (Count II); *Diaz v. Messer*, 742 F. App'x 250, 252 (9th Cir. 2018) (consent of all parties defeats a Section 632(a) claim) (Count II); *Oracle USA, Inc. v. Rimini Street, Inc.*, 879 F.3d 948, 962 (9th Cir. 2018) (CDAFA claim fails where defendant had authorization to take and use information at issue) (Count III); *Opperman v. Path, Inc.*, 205 F. Supp. 3d 1064, 1072 (N.D. Cal. 2016) (consent defeats claim of expectation of privacy) (Count IV & V); *Davis v. HSBC Bank Nevada, N.A.*, 691 F.3d 1152, 1169–71 (9th Cir. 2012) (disclosure defeats UCL claim) (Count VI).

1. The app developers voluntarily used GA for Firebase as a tool to collect their users' data and affirmatively authorized Google's collection.

In their first complaint, Plaintiffs alleged that app developers intentionally integrated GA for Firebase into their apps, fully aware that it automatically collects users' app activity data. *See* Compl. ¶ 33 ("Google itself explains to app developers [that] "Firebase's '[a]utomatically collected events are triggered by basic interactions with your app. As long as you use the Firebase SDK, you don't need to write any additional code to collect these events."). Citing the same source, the FAC similarly alleges that certain data is automatically collected "every time" a user interacts with an app. FAC ¶ 52–56. The GA for Firebase ToS also makes clear that app developers integrate Firebase into their apps in order to collect user's app activity data. For example, Firebase is defined in the ToS as "the Firebase Software Development Kit, which *is used or incorporated in an App for the purpose of collecting Customer Data*, together with any fixes, updates and *upgrades* provided You." The GA for Firebase Use Policy also makes clear that by subscribing to Google's Firebase service, app developers authorize Google to collect and use their users' app activity data: "[b]y enabling Google Analytics for Firebase you enable the collection of data about App Users, including via identifiers for mobile devices (including Android Advertising

ID and Advertising Identifier for iOS), cookies and similar technologies." *Id.*

Plaintiffs nonetheless contend in the FAC that the app developers did not consent to Google's collection of their users' data because Google told the apps that Google would comply with its own Privacy Policy. But Google did comply with that policy, which notifies both the app developers and users that "[m]any websites and apps use Google Analytics to understand how visitors engage with their sites or apps." Mitchell Decl. ¶ 15, and Ex. N; RJN ¶ 16. Further, based on the alleged facts, it defies credulity to claim that app developers voluntarily incorporated a tool into their apps meant to collect data about their users' interaction with their apps so that the data could be displayed by Google Analytics, yet somehow did not consent to the sending of that information *to Google*. And, if that weren't enough, the GA for Firebase Terms of Use and GA for Firebase Use Policy, both used with app developers, clearly delineate how GA for Firebase works. There is no question that the app developers knew what they were doing; that was the point.

Indeed, as Plaintiffs themselves allege in the FAC, Google disclosed to app developers that once GA for Firebase is integrated into an app, certain user data is *automatically* collected "*every time*" a user interacts with the app. FAC ¶ 55; *see also* Compl. ¶ 58 (alleging that Google's disclosures to apps make plain that Google-account-level settings, such as WAA, do not affect Firebase's data collection). In addition, Google explains to app developers that "in some cases, you may wish to temporarily or permanently disable collection of Analytics data, such as to collect end-user consent or fulfil legal obligations." Mitchell Decl. ¶ 16, and Ex. O; RJN ¶ 17.

Plaintiffs try to plead around these disclosures by alleging that "Google made significant efforts to coerce app developers to use Firebase SDK" and that "[d]evelopers often have no choice but to use Firebase SDK." FAC ¶¶ 42, 177. But Plaintiffs provide no factual basis for such "coercion," or why the apps would be forced to use a free product. Nor do they allege that app developers were coerced into using GA for Firebase; app developers using the Firebase SDK can choose not to employ GA for Firebase, even if they use other Firebase features. FAC ¶ 58. That developers find GA for Firebase useful does not make their adoption of it the product of coercion, and nothing in the complaint suggests any basis for this specious and conclusory allegation.

In any event, the alleged coercion does not change the voluntary authorization that users like Plaintiffs provided to the apps they used, and so cannot change that the use was authorized. *Cf. Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 117 (N.D. Cal. 2020). Plaintiffs failed to plead that Google lacked authorization to collect their app usage data for good reason: they cannot.

2. Google requires app developers to disclose the use of Google Analytics for Firebase to their users and to obtain their consent.

Section 7 of the GA for Firebase ToS, titled "Privacy," requires app developers to disclose their use of GA for Firebase to collect users' data and get users' consent:

> You must disclose the use of the [Firebase SDK] Service, and how it collects and processes data . . . . You will use commercially reasonable efforts to ensure that a User is provided with clear and comprehensive information about, and consents to, the storing and accessing of cookies or other information on the User's device where such activity occurs in connection with the Service and where providing such information and obtaining such consent is required by law.

Thus, as a condition of using Firebase to collect their users' information, app developers agreed to obtain consent to the collection, and the apps relevant here did so.

3. The app developers disclosed their use of Google Analytics for Firebase and required users to agree to the collection of their data.

As discussed above, apps using GA for Firebase are required to obtain consent from users, including Plaintiffs, to let Google collect their data, and indeed do so. Rope Decl. ¶ 2 & Ex. 1(a)–(b), pp. 5, 14. Consistent with the GA for Firebase ToS, app developers explicitly disclose the use of Google Analytics data collection and require users to consent to the collection of their data. For example, Alibaba's Privacy Policy discloses that Alibaba uses Google Analytics, and that data regarding users' page views and visiting history is transmitted to, and stored by, Google. Mitchell Decl. ¶ 3 & Ex. B(1)–(4); RJN ¶ 4. Lyft, NPR One, NYT, Trivago, Duolingo, and The Economist apps' privacy policies similarly disclose that they collect user data through Google Analytics to understand users' navigation behavior and response to advertisements. *See* Mitchell Decl. ¶¶ 6–7, 10–13; RJN ¶¶ 7–8, 11–14. Wattpad and Venmo disclose that third-parties use "cookies," which automatically collect data, on Wattpad's Sites and also discloses that Wattpad shares users' data with third-parties, including "Analytics providers." Mitchell Decl. ¶ 8, 13; RJN ¶ 9, 14.

The apps' privacy policies are incorporated into their terms of service agreements, which users must consent to in order to use the apps. *See supra* § II(C). Thus, in addition to the app developers authorizing Google to access data from the use of their apps, the users themselves (including Plaintiffs) consented, too. Because Plaintiffs consented to the collection of the data that forms the basis of each claim, the Complaint should be dismissed in its entirety with prejudice.

Plaintiffs argue that they did not consent to Google's collection of their data, or somehow withdrew their consent, because Google did not tell them their data was still being collected from apps using GA for Firebase when WAA was turned off. But Plaintiffs plainly consented to GA for Firebase through the apps, and they provide no explanation for why turning off an unrelated setting that performs a different function for a different reason would "withdraw" consent they gave to the apps. Plaintiffs' lack-of-consent theory is built out of suppositions and implications and is contrary to the express consent they provided.

Finally, nowhere do Plaintiffs allege that they saw the disclosures that form the basis of their lawsuit before their data was collected by app developers using Firebase. Instead, Plaintiffs argue generally that "users" expected that Google would stop collecting app data when WAA was turned off, without any specific factual allegation to support that assertion. *See, e.g.*, FAC ¶ 202.

B. Plaintiffs fail to state a claim under the Federal Wiretap Act because the app developers (and users) provided consent (Count I).

Plaintiffs allege that Google intercepted their communications with apps in violation of the federal Wiretap Act, 18 U.S.C. § 2510, *et seq*. FAC ¶ 122. As relevant here, to prove a violation of section 2511(1)(a), a plaintiff must show the (1) intentional (2) interception of (3) a wire, oral, or electronic communication. 18 U.S.C. § 2511(1)(a); *see also Backhaut v. Apple Inc.*, 148 F. Supp. 3d 844, 849 (N.D. Cal. 2015), *aff'd*, 723 F. App'x 405 (9th Cir. 2018).

The claim fails out of the gate because a single party's consent is fatal to the wiretap claim, and here the app developers consented. *See In re Yahoo Mail Litig.*, 7 F. Supp. 3d at 1026 (quoting 18 U.S.C. § 2511(2)(d)); *Murray v. Fin. Visions, Inc.*, CV-07-2578-PHX-JM, 2008 WL 4850328, at *4 (D. Ariz. Nov. 7, 2008). Here, the app developers provided consent by agreeing to the GA for Firebase Use Policy and integrating GA for Firebase into their apps for the express

purpose of sending user data to Google for analysis. Their consent defeats this claim. *See In re Yahoo Mail Litig.*, 7 F. Supp. 3d at 1026. (one-party consent is a "complete defense"). [2]

C. Plaintiffs fail to state a claim under CIPA (Count II).

Plaintiffs allege that Google violated Sections 631 and 632 of the California Invasion of Privacy Act ("CIPA"). Both the Section 631 and 632 claims fail because Plaintiffs consented to Google's collection of the data. And the Section 632 claim fails because Plaintiffs have not plausibly alleged an "invasion" by Google or an actionable privacy interest.

1. The Section 631 and 632 claims fail because Plaintiffs consented to Google's collection of the data.

"The California Supreme Court has held that Section 631 protects against three distinct types of harms: 'intentional wiretapping, willfully attempting to learn the contents or meaning of a communication in transit over a wire, and attempting to use or communicate information obtained as a result of engaging in either of the two previous activities.'" *In re Yahoo Mail Litig.*, 7 F. Supp. 3d at 1036. Consent of the parties to the communication is a complete defense to a Section 631(a) claim. *See Matera v. Google Inc.*, No. 15-CV-04062-LHK, 2016 WL 5339806, at *7 (N.D. Cal. Sept. 23, 2016) ("Under CIPA, a consent defense is established when both parties—the sender and the recipient of the communication— consent to the alleged interception."); *see also In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d at 607 (citing Cal. Pen. Code § 631(a) ("CIPA prohibits any person from using electronic means to 'learn the contents or meaning' of any 'communication' 'without consent' or in an 'unauthorized manner.'")).

"Section 632 is part of California's invasion of privacy statutory scheme. It provides, in relevant part, that "'[e]very person who, intentionally and without the consent of all parties to a confidential communication, by means of any electronic . . . device . . . records the confidential communication' violates the statute." *Weiner v. ARS Nat'l Servs., Inc.*, 887 F. Supp. 2d 1029,

[2] The FAC alleges that Google embeds secret software code or scripts into Firebase that copies and sends data to Google unbeknownst to the apps when WAA is off. FAC ¶ 44. This argument is as nonsensical as it is implausible. It makes no sense that Google would rely on secret codes in Firebase to collect app data when the app developers integrated Firebase into their apps for the very purpose of allowing Google to collect app data and provide analytics services.

1032 (S.D. Cal. 2012) (citing Cal. Pen. Code § 632(a)). "Accordingly, the three elements that Plaintiff must prove are (1) an electronic recording of (or eavesdropping on); (2) a 'confidential' communication; and (3) all parties did not consent." *Id.* (citing *Flanagan v. Flanagan*, 27 Cal. 4th 766, 774–76, 117 Cal. Rptr. 2d 574 (2002)).

Plaintiffs have failed to, and cannot, plead that all parties to the alleged communications (i.e. Plaintiffs and the apps) did not consent to Google's conduct. Both the app developers and users, including Plaintiffs, specifically consented to the collection of the underlying data. *See supra* § IV(A)(1)–(3). Plaintiffs' Section 632 claim thus fails as a matter of law and should be dismissed. *See, e.g., Maghen v. Quicken Loans Inc.*, 94 F. Supp. 3d 1141, 1146 (C.D. Cal. 2015), *aff'd in part, dismissed in part*, 680 F. App'x 554 (9th Cir. 2017) (section 632 claim failed because the parties to communication consented to defendant's conduct).

2. GA for Firebase is an "electronic means," not a "person" who invaded any Plaintiff's privacy.

The CIPA claim also fails because the FAC fundamentally alleges that GA for Firebase is the "electronic means" or "device" that the apps use to "record" the communications at issue. It is a tool, and Google requires it be used with consent, which the apps obtain. The app developers agree to those terms and employ GA for Firebase to learn about and analyze how their customers use their apps. GA for Firebase--like a dictaphone--cannot face liability under Plaintiffs' CIPA claims. *Cf.* Cal. Penal Code 631(a), 632(a) ("any ***person*** who . . .).

3. Plaintiffs failed to allege that their interactions with apps were confidential under Section 632.

Plaintiffs' Section 632 claim also fails because they do not plausibly allege what information was collected and accordingly how they expected that the information was confidential. Under Section 632, "a conversation is confidential if a party to that conversation has an objectively reasonable expectation that the conversation is not being overheard." *Cline v. Reetz-Laiolo*, 329 F. Supp. 3d 1000, 1051 (N.D. Cal. 2018) (citing *Flanagan*, 27 Cal. 4th at 766); *see also Flanagan* 27 Cal. 4th at 772–73 (adopting the confidentiality test set out in *Frio v. Superior Court*, 203 Cal. App. 3d 1480, 1488, 250 Cal, Rptr. 819 (1988)). This test is objective.

Id. Plaintiffs' subjective expectation of privacy is irrelevant to the inquiry. *Id.* at 766–77*; Coulter v. Bank of America Nat'l Tr. & Savings Ass'n,* 28 Cal. App. 4th 923, 929, 33 Cal. Rptr. 2d 766 (1994) ("the test of confidentiality is objective" and a party's subjective intent is irrelevant). In deciding whether a communication is confidential under Section 632, courts consider the "surrounding circumstances to determine whether the parties had an objectively reasonable expectation that the conversation is not being recorded or overheard." *Faulkner v. ADT Sec. Servs., Inc.*, No. C 11-00968 JSW, 2011 WL 1812744, at *3 (N.D. Cal. May 12, 2011) (citing *Flanagan*, 27 Cal. 4th at 776–77 (collecting cases)).

Here, Plaintiffs have not plausibly alleged that the data they shared was objectively confidential. Rather, they imply they did not expect Google to collect it because they had turned off WAA. *See, e.g.*, FAC ¶¶ 75, 246 ("[T]he communications intercepted by Google were plainly confidential, which is evidenced by the fact that Plaintiffs . . . turned off 'Web & App Activity."). Plaintiffs further allege that the "contents" of the allegedly confidential communications were "detailed URL requests, app browsing histories, and search queries." FAC ¶ 241. Plaintiffs allege that the communications between app users and app developers that are collected via Firebase contain "personally identifiable information," and were "confidential," but provide no factual allegations in support. *Id.* ¶¶ 45, 246.

These allegations fail to state a Section 632 claim. Plaintiffs must allege that the information they shared with the apps is confidential and provide facts supporting those allegations. *See In re Gilead,* 536 F.3d at 1055 (The court may reject "conclusory, unwarranted deductions of fact, or unreasonable inferences." It is not enough for Plaintiffs to allege that they did not expect *Google* to collect the information (setting aside that they consented to it). Nor does their bald and unsupported assertion that the information was confidential hold water. *See, e.g., In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797, 817 (N.D. Cal. 2020) (citing *Sunbelt Rentals, Inc.*, 43 F. Supp. at 1035 (finding that certain electronic communications were not confidential within the meaning of Section 632)); *see also Revitch v. New Moosejaw, LLC*, No. 18-cv-06827-VC, 2019 WL 5485330 (N.D. Cal. Oct. 23, 2019) (same).

Plaintiffs barely plead what data may have been collected and only identify data showing the title of the app page they visited, whether they arrived at that page from another page, and the page URL. (FAC ¶¶ 55, 244.) Plaintiffs also generally allege that data collected by Firebase contained personally identifiable information but fail to identify what specific personally identifiable data Google allegedly collected. The answer is none: the GA for Firebase ToS and Use Policy forbid apps from sharing users' personally identifiable information with Google. Rope Decl. ¶ 2 and Ex. 1(a)-(b), pp. 4, 14; *id.* ¶ 3 and Ex. 2(a)–(b), pp. 1, 3. Google also instructs app developers to ensure that the IDs that apps use to refer to their users "not contain any information that a third party could use to determine the identity of an individual user." Mitchell Decl. ¶ 14, and Ex. M; RJN ¶ 15. Plaintiffs' allegation should thus be disregarded as it is conclusory and at odds with judicially noticeable documents. *See Cotti v. Pa Chang,* No. 18-CV-02980-BLF, 2020 WL 2572771, at *12 (N.D. Cal. May 21, 2020) ("The court need not accept conclusory allegations . . . that are unsupported by the facts alleged in the complaint." (citing *Newt v. Kasper,* 85 F. App'x 37, 38 (9th Cir. 2003)); *see also Sprewell v. Golden State Warriors,* 266 F.3d 979 (9th Cir. 2001) (holding that for purposes of 12(b)(6) motion, conclusory allegations need not be accepted as true). Accordingly, Plaintiffs have failed to allege the communications at issue were objectively confidential.

D. Plaintiffs fail to state a claim for invasion of privacy under the California Constitution and common law intrusion upon seclusion (Counts IV & V).

To state a claim for invasion of privacy under the California Constitution, "Plaintiff must show that: (1) they possess a legally protected privacy interest, (2) they maintain a reasonable expectation of privacy, and (3) the intrusion is 'so serious … as to constitute an egregious breach of the social norms' such that the breach is 'highly offensive.'" *In re Facebook, Inc. Internet Tracking Litig.*, 956 F. 3d at 601 (quoting *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 286 (2009)). To state a claim for inclusion upon seclusion, Plaintiffs must establish: (a) an intrusion into a private place, conversation, or matter, (b) in a manner highly offensive to a reasonable person. *See In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797, 828 (N.D. Cal. 2020). Because of the similarity in the tests for common law and Constitutional invasion of privacy

claims, "courts consider the claims together and ask whether: (1) there exists a reasonable expectation of privacy, and (2) the intrusion was highly offensive." *In re Facebook, Inc., Internet Tracking Litig.*, 956 F. 3d at 601. Plaintiffs fail to plausibly plead either of these elements.

1. Plaintiffs fail to allege an actionable privacy interest.

As discussed above, because Plaintiffs consented to Google receiving data concerning their use of apps that incorporated Google Analytics for Firebase, and because they have not sufficiently alleged that any of the data are confidential, Plaintiffs have not plausibly alleged that Google violated their reasonable expectation of privacy. *First*, Plaintiffs consented to Google receiving the underlying data (*see supra* § II(A)(1)–(3)), which obviates a reasonable expectation of privacy in that information. *See Smith v. Facebook, Inc.*, 262 F. Supp. 3d 943, 955–56 (N.D. Cal. 2017) (plaintiffs' consent bars common law and constitutional privacy claims); *In re Yahoo Mail Litig.*, 7 F. Supp. 3d at 1037–38 (holding that a plaintiff asserting a privacy claim under the California Constitution "must not have manifested by his or her conduct a voluntary consent" to defendant's conduct) (quoting *Hill*, 7 Cal. 4th at 26). *Second*, as explained above, Plaintiffs fail to plausibly allege that the information Google allegedly collected is objectively confidential--they fail to explain why their app usage constitutes "personally identifiable information" or how it is otherwise confidential. Plaintiffs have thus failed to allege information upon which a common law or constitutional invasion of privacy claim can be based. *Cf. Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal 2012) (plaintiffs did not adequately state a claim for common law or constitutional invasion of privacy where they did not allege that anyone "de-anonymize[d]" their "browsing history" data even if it could be de-anonymized).

2. Plaintiffs fail to allege a highly offensive invasion of privacy that constitutes an egregious breach of social norms.

Even if Plaintiffs had alleged an actionable privacy interest, they still have not alleged an invasion of privacy that is actionable. The "California Constitution … set[s] a high bar for an intrusion to be actionable." *In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d at 830 (citation and quotation marks omitted). Plaintiffs have failed to plausibly allege that Google receiving

users' basic app activity data constitutes a "highly offensive" invasion of privacy or "an egregious breach of social norms."

As a preliminary matter, there was no "invasion" by Google at all—the apps used GA for Firebase as a tool to analyze their users' information. Nor does the fact that apps used GA for Firebase to collect data regarding users' activity within an app constitute an "egregious breach of social norms" under the California constitution. Courts in this district have made clear that collection of the type of information at issue in this case is routine commercial behavior that does not give rise to a "highly offensive" invasion of privacy. *See, e.g., In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1050, 1063 (N.D. Cal. 2012); *Moreno v. San Francisco Bay Area Rapid Transit Dist.*, No. 17-cv-02911-JSC, 2017 WL 6387764, at *8 (N.D. Cal. Dec. 14, 2017) (accessing anonymous data from an app, even when the app is not in use, would not be highly offensive or egregious to a reasonable user); *Yunker v. Pandora Media, Inc.*, No. 11-CV-03113 JSW, 2013 WL 1282980, at *15 (N.D. Cal. Mar. 26, 2013) (no actionable privacy violation where the Pandora app collected plaintiff's PII and provided that information to advertisers); *Low*, 900 F. Supp. 2d at 1015 (LinkedIn did not commit a "highly offensive" invasion of users' privacy by disclosing users' browsing histories to third parties); *In re Google, Inc. Privacy Policy Litig.*, 58 F. Supp. 3d 968, 988 (N.D. Cal. 2014) (Google's collection and disclosure of users' data, including their browsing histories, "do not plausibly rise to the level of intrusion necessary to establish an intrusion claim."); *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1063 ("[D]isclos[ure] to third parties [of] … unique device identifier number, personal data, and geolocation information from Plaintiffs' iDevices … does not constitute an egregious breach of social norms." (citation omitted)).[3]

[3] Indeed, the type of conduct that meets this element is a far cry from what is alleged here. *See Susan S. v. Israels*, 55 Cal. App. 4th 1290, 1298, 67 Cal. Rptr. 2d 42, 47 (1997) ("stranger's unauthorized reading and dissemination of a person's mental health records is a serious invasion of the person's privacy."); *Givens v. Regents of Univ. of Cal.*, No. G030663, 2003 WL 21246766 (Cal. Ct. App. May 30, 2003) (disclosure of an employee's whistleblower status violated the employee's constitutional right of privacy).

E. Plaintiffs fail to state a claim under CDAFA, Cal. Pen. Code § 502(c) (Count III).

Plaintiffs fail to state a claim against Google for violation of the Comprehensive Computer Data Access and Fraud Act ("CDAFA") because: (a) Google was authorized to access Plaintiffs' app activity data, and (b) Plaintiffs have not alleged that Google circumvented any technical or code-based barriers to access the data. CDAFA prohibits "knowingly accessing, and without permission, using any data, computer, computer systems, or computer network" in certain prohibited ways. Cal. Pen. Code § 502. To adequately plead that a party acted "without permission" under CDAFA, a plaintiff must allege that defendant "circumvent[ed] technical or code-based barriers in place" to prevent unauthorized access. *See Williams v. Facebook, Inc.*, 384 F. Supp. 3d 1043, 1053 (N.D. Cal. 2018). Plaintiffs' claims fail because (1) Google was authorized to access Plaintiffs' app activity data; and (2) Plaintiffs have not alleged that Google circumvented any technical or code-based barriers to access the data.

First, Google was authorized by both the app developers and the users to access and use the information at issue. *See Oracle USA, Inc.* 879 F.3d at 962 (holding that plaintiffs cannot state a claim under CDAFA where the defendant had authorization to take and use the information upon which the CDAFA claims is based); *see also Brodsky*, 445 F. Supp. 3d at 131–32 (dismissing CDAFA claim because defendant had authorization to access plaintiffs' data). Google's access to the data therefore was not "without permission."

Second, Plaintiffs do not allege that Google accessed their app activity data by circumventing "technical or code-base barriers." FAC ¶¶ 264–273. Instead, Plaintiffs merely allege that Google acquired Plaintiffs' sensitive personal information in contravention of "Google's false representations to the contrary." FAC ¶ 267. But section 502 requires efforts to circumvent technical or code-based barriers, which are never alleged here. *See, e.g., In re iPhone Application Litig.*, No. 11-MD-02250-LHK, 2011 WL 4403963, at *10 (N.D. Cal. Sept. 20, 2011) (citing Cal. Pen. Code § 502); *see also In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 716 (N.D. Cal. 2011) ("It is thus impossible, on Plaintiffs' own allegations, for Defendant to be liable

under the subsections of Section 502 which require a defendant to act 'without permission,' as there were clearly no technical barriers blocking Defendant from accessing its own website.").

Nor is it plausible that Google "circumvented" technical, code-based or any other barriers, because, as explained above, the apps authorized Google to collect the information *using Firebase*, a tool developers intentionally integrated into their apps for that very purpose. *See* FAC ¶ 51, n.14 (Google discloses to app developers that "Firebase '[a]utomatically collected events are triggered by basic interactions with your app. As long as you use the Firebase SDK, you don't need to write any additional code to collect these events."). Thus, not only have Plaintiffs failed to allege any facts from which the Court could conclude that Google "circumvented" technical or code-based barriers, but such an allegation would also be facially implausible in light of the remainder of the allegations contradicting such an inference.

F. Plaintiffs lack UCL standing and fail to state a UCL claim (Count VI).

Plaintiffs' UCL claim fails because Plaintiffs fail to plead: (1) that they suffered a cognizable injury in fact and have thus failed to plead that they have statutory standing under the UCL; (2) a predicate offense that can underlie the unlawful prong claim; and (3) any independent basis for the unfair prong claim.

1. Plaintiffs fail to plead UCL standing.

A private person has standing to bring a UCL claim only if he or she "has suffered injury in fact *and* has lost money or property as a result of the unfair competition." *Durell v. Sharp Healthcare*, 183 Cal. App. 4th 1350, 1359 (2010) (emphasis added). Accordingly, to establish UCL standing, a plaintiff must establish "*economic injury*" that was the result of, i.e., *caused by*, the unfair business practice alleged. *Id.* (emphasis in original). The UCL standing requirement is more stringent than the federal Article III standing requirement; "whereas a federal plaintiff's 'injury in fact' may be intangible," a UCL plaintiff's may not be. *Troyk v. Farmers Grp., Inc.*, 171 Cal. App. 4th 1305, 1348, n.31 (2009). Plaintiffs' allegations do not meet these requirements.

First, Plaintiffs allege that they paid consideration when they agreed to Google's Privacy Policy. They do not (and cannot) allege that this "consideration" was money or other property as

required by the UCL. Nor can they establish causation, because they do not (and cannot) allege that they lost money or property *because of* the alleged violations of Google's Privacy Policy.

Second, Plaintiffs allege that they paid money for the third-party apps. But they don't allege they paid that money to *Google*, as required to establish UCL standing as to Google. *See* FAC ¶¶ 39–40; *Cf. In re iPhone Application Litig.*, 2011 WL 4403963, at *1–2 (UCL plaintiffs lacked standing to sue Apple for allowing third-party apps to collect personal information without consent for advertising and analytics). In In iPhone Application Litigation, the plaintiffs brought a UCL claim against Apple for allowing third-party apps to collect user data for advertising and analytics purposes. Id. at *1–2. The Court found that the plaintiffs lacked UCL standing because, even if they paid for the apps they downloaded, they didn't pay it to Apple. *See id.*

Third, Plaintiffs allege that Google's collection of their data deprived them of a property interest or diminished the economic value of that property. FAC ¶ 313. This is insufficient to plead that Plaintiffs lost money or property for purposes of the UCL. Plaintiffs allege that the data at issue is personal information (FAC ¶ 267), but "[n]umerous courts have held that a plaintiff's 'personal information' does not constitute money or property under the UCL." *In re iPhone Application Litigation*, 2011 WL 4403963, at *14.[4] Courts have also found that unauthorized release of personal information is not a loss of property under the UCL. *See, e.g., Ruiz v. Gap, Inc.*, 540 F. Supp. 2d 1121, 1127 (N.D. Cal 2008) (finding no "authority to support the contention

[4] *See also In re Facebook, Inc., Consumer Privacy User Profile Litig.*, 402 F. Supp. 3d 767, 784 (N.D. Cal. 2019) (plaintiffs failed to allege Article III or UCL standing in privacy claim because "although it's true that each user's information is worth a certain amount of money to Facebook and the companies Facebook gave it to, it does not follow that the same information, when not disclosed, has independent economic value to an individual user."); *Opperman v. Path, Inc.*, 87 F. Supp. 3d 1018, 1058 (N.D. Cal. 2014) (plaintiffs failed to allege UCL standing because alleged theft of a virtual address book by a third party app did not cause the loss of money or property); *In re Google, Inc. Privacy Policy Litig.*, No. C-12-01382-PSG, 2013 WL 6248499, at *5 (N.D. Cal. Dec. 3, 2013) ("[I]njury-in-fact in this context requires more than an allegation that a defendant profited from a plaintiff's personal identification information. Rather, a plaintiff must allege how the defendant's use of the information deprived the plaintiff of the information's economic value. Put another way, a plaintiff must do more than point to the dollars in a defendant's pocket; he must sufficiently allege that in the process he lost dollars of his own."); *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 715 (N.D. Cal. 2011) (rejecting UCL claim because "personal information" is not a form of property under the UCL).

that unauthorized release of personal information constitutes a loss of property").

Plaintiffs also allege that they had "property interest" and "value" in the anonymized app data that Google allegedly collected. FAC ¶ 313. This allegation fares no better because "property value in one's information[] do[es] not suffice as an injury in fact under the UCL." *In re Sony Gaming Networks and Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 966 (S.D. Cal. 2012); see also In re iPhone Application Litig., 2011 WL 4403963, at *14 (personal information is not a form of property under the UCL); *Low*, 900 F. Supp. 2d, at 1030 ("[A] plaintiff's 'personal information' [including browsing histories] does not constitute property.")

Accordingly, Plaintiffs have failed to plead that Google's conduct caused Plaintiffs any economic injury, within the meaning of the UCL, and thus fail to plead that they have statutory standing to bring a UCL claim.

2. Plaintiffs fail to state a UCL claim based on the "unlawful" prong.

Plaintiffs predicate their unlawful prong claim on Google's alleged violations of the Federal Wiretap Act, CIPA, §§ 631, 632, CDAFA, the California Constitution, Art. I, and the rights of privacy and seclusion. FAC ¶ 307. However, unlawful prong claims cannot be predicated on any of these alleged offenses because they fail as independent causes of action, as explained above. *See Hadley v. Kellogg Sales Co.*, 243 F. Supp. 3d 1074, 1094 (N.D. Cal. 2017); *Metro Publ'g., Ltd. v. San Jose Mercury News, Inc.*, 861 F. Supp. 870, 881 (N.D. Cal. 1994); *Punian v. Gillette Co.*, No. 14-CV-05028-LHK, 2016 WL 1029607, at *17 (N.D. Cal. Mar. 15, 2016); *Fabozzi v. Stubhub, Inc.*, No. C-11-4385 EMC, 2012 WL 506330, at *5 (N.D. Cal. Feb. 15, 2012).

The unlawful prong claim is also predicated on the FTC Act, the FTC settlement agreement with Google, California Business & Profession Code § 22576, and the CCPA. FAC ¶ 307. None of these predicate offenses is a cognizable basis for an unlawful prong claim.

First, the FAC does not contain factual allegations sufficient to establish a violation of the FTC Act, Cal. Bus. Code § 22576, or the CCPA, as is required to adequately plead a UCL unlawful prong claim. *See Aquino v. Credit Control Servs.*, 4 F. Supp. 2d 927, 930 (N.D. Cal. 1998) (dismissing UCL action where plaintiffs failed to "set forth any factual allegations that the defendant's approach violated any state or federal provisions"); *see also Silicon Knights, Inc. v.*

Crystal Dynamics, Inc., 983 F. Supp. 1303, 1316 (1997) ("A plaintiff alleging unfair business practices under the unfair competition statutes 'must state with reasonable particularity the facts supporting the statutory elements of the violation.'" (citing *Khoury v. Maly's of Cal.*, 14 Cal. App. 4th 612, 619, 17 Cal. Rptr. 2d 708, 712 (1993))). The FAC does not explain what sections of the FTC Act or the CCPA statutes Google allegedly violated, much less allege factual allegations supporting their statutory elements.

Second, the alleged violation of the FTC consent order, which is a settlement agreement with Google, is not a cognizable predicate for an unlawful prong claim. *Cf. Newton v. American Debt Services, Inc.*, 75 F. Supp. 3d 1048 (N.D. Cal. 2014) (violation of an FDIC consent order cannot form the basis of a UCL unlawful or unfair prong claim). Google did not admit liability and a consent order "does not establish illegal conduct"; violation of such an order therefore cannot constitute unlawful conduct. *See Intergraph Corp. v. Intel Corp.*, 253 F.3d 695, 698 (Fed. Cir. 2001). Plaintiffs' insinuation that violation of the consent order is *ipso facto* a violation of the FTC Act is also wrong for the same reason. FAC ¶ 307.

Third, the FTC Act and CCPA expressly preclude private enforcement and cannot be a predicate offense under the UCL. *See Hartless v. Clorox Co.*, No. CIV. 06CV2705JAHCAB, 2007 WL 3245260, at *4 (S.D. Cal. Nov. 2, 2007) ("A private right of action under the unlawful prong of the UCL will be forestalled if the predicate statute actually bars the private action."). The FTC Act "doesn't create a private right of action, and plaintiffs can't use California law to engineer one." *O'Donnell v. Bank of Am., Nat'l Ass'n*, 504 F. App'x 566, 568 (9th Cir. 2013). And the CCPA cannot be used as a predicate for private rights of action under other statutes such as the UCL. *See* Cal. Civ. Code § 1798.150(c) ("Nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law."); *see also* Senate Judiciary Committee Report, AB-375, 2017–2018 Sess. (Cal. 2018) (noting that Cal. Civ. Code § 1798.150(c) "would eliminate the ability of consumers to bring claims for violations of the Act under statutes such as the Unfair Competition Law, Business and Professions Code Section 17200 *et seq.*"). In any event, the CCPA expressly bars private enforcement except in the limited circumstances enumerated in section 1798.150(a)(1), none of which are applicable here.

3. The FAC does not state an "unfair" prong UCL claim.

Despite the fact that app developers intentionally integrated GA for Firebase into their apps, and that users consented to the use of GA for Firebase to improve those apps, Plaintiffs allege in conclusory fashion that Google's conduct was "immoral, unethical, oppressive," etc. FAC ¶¶ 308–10. But Plaintiffs allege that their unfair prong claim is tethered to the same statutes upon which their unlawful prong claim is predicated, and so it fails for the same reasons.[5] *See Punian*, 2016 WL 1029607, at *17 (dismissing unfair prong claim where it "overlaps entirely" with meritless unlawful prong claim).

As for Plaintiffs' bare accusations of immoral behavior and consumer injury, nothing in the FAC can support these allegations. As discussed in connection with other claims, the FAC has not alleged any wrongdoing of any kind. Google made a data analysis tool available to app developers. App developers of all kinds integrated that tool into their apps. They obtained the consent of users to employ the tool. And Plaintiffs turned off WAA, which stopped the storage of those users' activity on certain *Google* products and services The complaint states no allegation that could support a finding of unfairness.

V. CONCLUSION

For these reasons, Google respectfully requests that the Court dismiss Plaintiffs' First Amended Complaint in its entirety with prejudice.

Dated: December 17, 2020

Respectfully submitted,

WILLKIE FARR & GALLAGHER LLP

By: /s/ *Benedict Y. Hur*

Benedict Y. Hur

[5] Though it is possible for the unfair prong to reach farther than those statutes, the utter lack of merit of the claims under those statutes in juxtaposition with Plaintiffs' bare allegations of conclusions of law dictate dismissal here.